Scope and Goals of the Audit

Scope:

- The audit scope is appropriately comprehensive, covering the entire security program at Botium Toys. This includes all physical, technical, and administrative aspects of the organisation's IT infrastructure and data management.

Goals:

- The primary goal is to assess existing assets and complete the controls and compliance checklist to identify necessary improvements in Botium Toys' security posture.
- The audit aims to evaluate current controls, identify gaps, and ensure compliance with U.S. and international regulations.

Current Assets

Assets Managed:

- On-premises equipment and end-user devices
- Storefront products and warehouse inventory
- Management systems (accounting, telecommunication, database, security, e-commerce, inventory management)
- Internet access and internal network
- Data retention and storage
- Legacy system maintenance

Risk Assessment

Risk Description:

- The key risk is inadequate management of assets and insufficient controls leading to non-compliance with regulations. The company is exposed to potential data breaches, legal penalties, and operational disruptions due to these gaps.

Risk Score:

- The risk score of 8 out of 10 indicates a high level of risk due to the lack of controls and compliance practices.

Additional Comments:

- **Access Controls:** Lack of least privilege and separation of duties increases the risk of insider threats and unauthorized access to sensitive data.
- **Encryption:** Absence of encryption for customer credit card information jeopardizes data confidentiality and compliance with data protection regulations.

- **Disaster Recovery & Backups:** The absence of disaster recovery plans and backups poses a significant risk to business continuity.
- **Compliance with E.U. Regulations:** The company has established a breach notification plan and privacy policies, but needs to address other compliance gaps, such as encryption and data access controls.

Review of Controls and Compliance Checklist

Administrative/Managerial Controls:

1. **Least Privilege (Preventative):**
    - Not implemented. Risk of unauthorized access and insider threats is high.
2. **Disaster Recovery Plans (Corrective):**
    - Not in place. Business continuity is at risk in the event of a disaster or system failure.
3. **Password Policies (Preventative):**
    - Existing policy is outdated. Needs updating to meet current complexity requirements.
4. **Access Control Policies (Preventative):**
    - Not implemented. Confidentiality and integrity of data are at risk.
5. **Account Management Policies (Preventative):**
    - Not specified. Managing account lifecycle and reducing attack surface are essential.
6. **Separation of Duties (Preventative):**
    - Not implemented. Increases risk of unauthorized access and misuse.

Technical Controls:

1. **Firewall (Preventative):**
    - Implemented. Effective at filtering unwanted or malicious traffic.
2. **IDS/IPS (Detective):**
    - Not implemented. Lack of detection for anomalous traffic increases vulnerability.
3. **Encryption (Deterrent):**
    - Not implemented for credit card information. Data confidentiality is at risk.
4. **Backups (Corrective):**
    - Not in place. Risk of data loss and inability to recover from incidents.
5. **Password Management (Preventative):**
    - Not centralized. Increases password fatigue and management overhead.
6. **Antivirus Software (Preventative):**
    - Implemented and monitored. Helps in detecting and quarantining threats.
7. **Manual Monitoring, Maintenance, and Intervention (Preventative):**
    - Implemented but lacks a regular schedule. Essential to manage system threats and vulnerabilities.

Physical/Operational Controls:

1. **Time-controlled Safe (Deterrent):**
    - Implemented. Helps protect sensitive physical assets.

2. **Adequate Lighting (Deterrent):**
    - Implemented. Reduces hiding places for potential threats.
3. **CCTV (Preventative/Detective):**
    - Implemented. Provides surveillance and can deter or document events.
4. **Locking Cabinets (Preventative):**
    - Implemented. Protects network gear from unauthorized access.
5. **Signage Indicating Alarm Service Provider (Deterrent):**
    - Implemented. Deters potential intruders by indicating security measures.
6. **Locks (Deterrent/Preventative):**
    - Implemented. Secures physical access to assets.
7. **Fire Detection and Prevention (Detective/Preventative):**
    - Implemented. Detects and prevents fire damage.

Recommendations

1. **Implement Least Privilege and Separation of Duties:**
    - Review and revise access controls to ensure that employees have only the necessary permissions for their roles.
2. **Update Password Policies:**
    - Align password policies with current best practices for complexity and enforce them through a centralized password management system.
3. **Establish Disaster Recovery and Backup Plans:**
    - Develop and document disaster recovery plans and ensure regular backups of critical data.
4. **Implement Encryption for Sensitive Data:**
    - Apply encryption for credit card information and other sensitive data both at rest and in transit.
5. **Deploy IDS/IPS:**
    - Implement an intrusion detection and prevention system to monitor and respond to network anomalies.
6. **Regularize Legacy System Maintenance:**
    - Establish a regular schedule for monitoring and maintaining legacy systems, and clarify intervention methods.
7. **Enhance Compliance with E.U. Regulations:**
    - Review and ensure compliance with all relevant E.U. data protection regulations, including encryption and data access controls.

By addressing these gaps and implementing the recommended controls, Botium Toys can improve its security posture, mitigate risks, and enhance its compliance with relevant regulations.